

# Mitigating The Impact Of A Data Investigation

By **Chris Riper, Michael Busen and Scott Sizemore** (November 27, 2019)

The U.S. Securities and Exchange Commission recently awarded \$1.8 million to a single whistleblower through the whistleblower program created by the 2010 Dodd-Frank Act. Since its first award in 2012, the SEC has awarded \$387 million under the program, including nearly \$60 million in 2019.[1][2]

It's a situation all companies want to avoid: A brewing scandal about the mishandling of data that begins first as rumors before exploding into public view, whether from a whistleblower who comes forward with damning evidence, or a regulator that obtains a misleading partial picture of the situation. More often than not the scandal will escalate, creating a public relations nightmare, and putting corporate executives and their boards on the back foot as they determine the best way to respond.

Forced into a highly reactive posture and without all the data, corporate executives may take multiple missteps. Initially, they may fail to understand the magnitude of the issue. Once they finally have a clearer grasp of the situation, they may not react quickly enough.

The financial fallout from the scandal may range from the millions to the billions. Regulatory scrutiny for highly regulated industries could increase substantially. However, most worrying for companies should be the sense of betrayal and loss of trust customers will feel, resulting in long-lasting reputational damage from which some companies may never recover.

## **Data is often at the heart of both the problem and the solution.**

In almost every instance, the data is both the source of the problem and the solution. Over the last several years, the adoption of big data within large corporations has skyrocketed as they seek to better understand their customers, competitors and themselves.

The amount of data being generated is staggering. It is estimated that by 2025, 463 exabytes, the equivalent of 212,765,957 DVDs, will be created each day.[3] Yet, for all the opportunities big data offers, there are significant risks for companies facing regulatory scrutiny or an internal investigation.

Cyberattacks, privacy breaches, use of customer data without consent, storing sensitive data on insecure or open networks, employee misuse of data, or failure to negotiate appropriate security standards with third-party cloud providers are only a few of the ways large corporations have been caught mishandling data — for which they have endured expensive investigations, hefty fines and consumer backlash.

The cost — not penalty for noncompliance — to comply with recent legislation like the EU's General Data Protection Regulation and the California Consumer Privacy Act to appropriately administer data and consumer preferences on that data has been estimated to be up to \$16.454 billion in the next 10 years.[4]



Chris Riper



Michael Busen



Scott Sizemore

As the volume and complexity of company data increases, large multinational corporations face particular challenges when subject to an investigation. Data relevant to the investigation is often siloed within a business unit or function, making the data difficult to identify, access or analyze.

### **Companies will want to look for ways to offset sanctions.**

When facing such daunting costs and potential penalties in litigation, it can be helpful to look at ways to offset the financial impact levied by the regulators by obtaining credit for extraordinary cooperation.

In July 2019, the Financial Industry Regulatory Authority updated its published guidance on credit for extraordinary cooperation and listed the following three examples that could result in such credit:

- Engage or conduct an independent audit or investigation that is thorough and far-reaching in scope beyond the immediate issue, with an eye toward identifying and remediating all related misconduct that may have occurred.
- Hire independent consultants to ensure the adoption and implementation of improved supervisory systems, procedures and controls.
- Where the root cause of a violation relates to organizational weaknesses — such as where a firm dedicated inadequate staff to the supervision of a particular business line — make organizational changes by, for example, creating new supervisory positions, adjusting reporting lines, or if necessary, removing or disciplining responsible individuals. This could include those in supervisory roles, although personnel changes are not necessarily required to achieve extraordinary cooperation.[5]

As to why a company would consider going to such lengths, FINRA outlined the potential benefit in the same updated guidance:

Enforcement may recommend a sanction that is well below the range set forth in the Sanction Guidelines or comparable precedents when respondents have voluntarily provided such material assistance to FINRA in its investigation, or effected such expedient and effective remediation, that FINRA deems these steps to constitute “extraordinary cooperation” beyond what it requires of any member firm or associated person.[6]

In our experience, this perspective is not held solely by FINRA and has been seen in the stances of other regulators as well.

### **Mitigate the impact of an investigation that involves data.**

Here are five tips for companies to consider that can maximize the benefit to the company while mitigating the impact of an investigation:

1. Appoint a qualified data consultant: The data consultant — whether an employee or third-party resource — can work with in-house or outside counsel, as well as company employees to determine the potentially relevant sources of company data, as well as where it lives, how it is managed and secured, and how it is disposed of.

2. Assign the right level of system access: Because of the siloed nature of many organizations, companies need to understand each group's data to blend the disparate data sources. As these groups generally use multiple systems, the company will have to allocate a secure area within the network to store the cross-enterprise data necessary for a complete analysis. With the right level of access, in-house and third-party team members can combine company data from disparate systems and perform analyses critical to the investigation, including analyses of key metrics, trends and identify so-called hot spots by geography, business unit, leadership and over specific periods of time.

3. Open the channels of communication: Give the investigation team access to appropriate levels of personnel across business units and functions so that they can attend and conduct interviews (especially when the subject requires technical expertise), quantify potential impacts to the company and its customers, and work with forensic accountants or company accounting, finance and audit personnel to determine impacts to records, financial reporting and internal controls.

4. Leverage stakeholder and regulator relationships: Companies will want to leverage relationships with regulators and other stakeholders to help present the results to affected stakeholders, such as describing the methods used to obtain, compile and analyze the data. More specifically, a data consultant will be well-positioned to liaise with the regulator's own data consultants to help navigate more technically focused conversations and respond to regulator requests for data.

5. Establish processes that move the company from reactive to proactive: Once the investigation is complete, companies will want to calculate remediation and work to establish ongoing processes that can place the company on more proactive footing so that a similar situation can be avoided in the future.

**Make sure there is no next time.**

No executive, general counsel or board wants their company's name splashed across media headlines as part of a data scandal. Whether the financial cost is millions or billions, the reputational cost is often so much more.

In an ideal world, the company would have processes, procedures and metrics in place to identify small issues before they get big, or avoid even small issues from forming.

However, once the proverbial scandal train has left the station, senior executives, general counsel or the board and its outside legal counsel will want to make certain they employ best practices to help the company navigate its labyrinth of data throughout an investigation.

---

*Chris Riper, Michael Busen and Scott Sizemore are managing directors in the forensic and litigation group at FTI Consulting Inc.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

*Posted with permission from Law360 ©2019 Portfolio Media, Inc. All rights reserved*

[1] <https://www.sec.gov/news/press-release/2019-165>.

[2] <https://www.sec.gov/whistleblower/pressreleases>.

[3] <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>.

[4] [https://oag.ca.gov/system/files/attachments/press\\_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf](https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf).

[5] "Regulatory Notice 19-23: FINRA Supplements Prior Guidance on Credit for Extraordinary Cooperation," FINRA, [finra.org](http://finra.org), © 2019 FINRA. All Rights Reserved. <https://www.finra.org/rules-guidance/notices/19-23>.

[6] Ibid.